
University of Padua – Department of Information Engineering
Bachelor's Degree in Computer Engineering

Final Report
***«Design and implementation of a SAML-based SSO
authentication component»***

Supervisor: Prof. Damiano
Varagnolo

Student's name: Ferro Simone
Student ID: 2066607

Padua, 21/7/2026

THE OBJECTIVE

Context: Exerplaza is an existing application

Goal:

- *Introduce SAML2-based Single Sign-On capability*

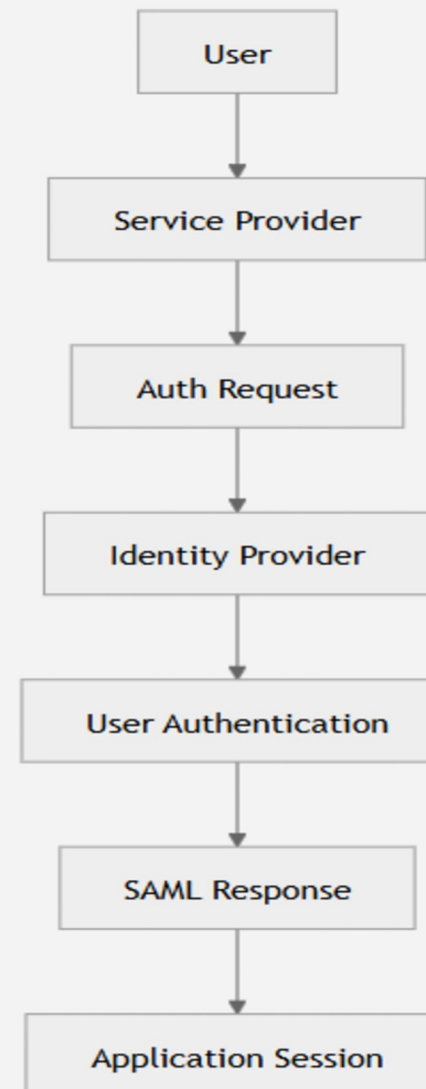
Requirements:

- *Reliable authentication flow*
- *Compatibility with existing behaviour*
- *Minimal architectural disruption*

Saml2 allows application to delegate authentication to an external Identity Provider

*Service Provider (SP) :
Application requesting authentication*

*Identity Provider (IDP):
System responsible for authentication*



Exerplaza is a deployed application with:

- *Existing authentication system*
- *Existing user/session management*
- *Deeply integrated with python logic*

Result:

- *Invasive changes are costly*

Approach 1

Application-level Saml2 integration

- *Python based*
- *Built on existing infrastructure*

Approach 2

Dedicated Saml2 Service Provider

- *Separate Authentication Component*
- *Separate infrastructure*

Evaluation criteria:

- *Integration effort*
 - *maintainability*
 - *Architectural fit*

Dedicated Saml2 service provider required:

- *Additional infrastructure*
- *Higher architectural impact*

*Replacement of existing authentication system was too disruptive
Integration was chosen instead of replacement*

Chosen solution:

Python-integrated Saml2 using Pyasml2 library

~~ExerPlaza~~ Log In

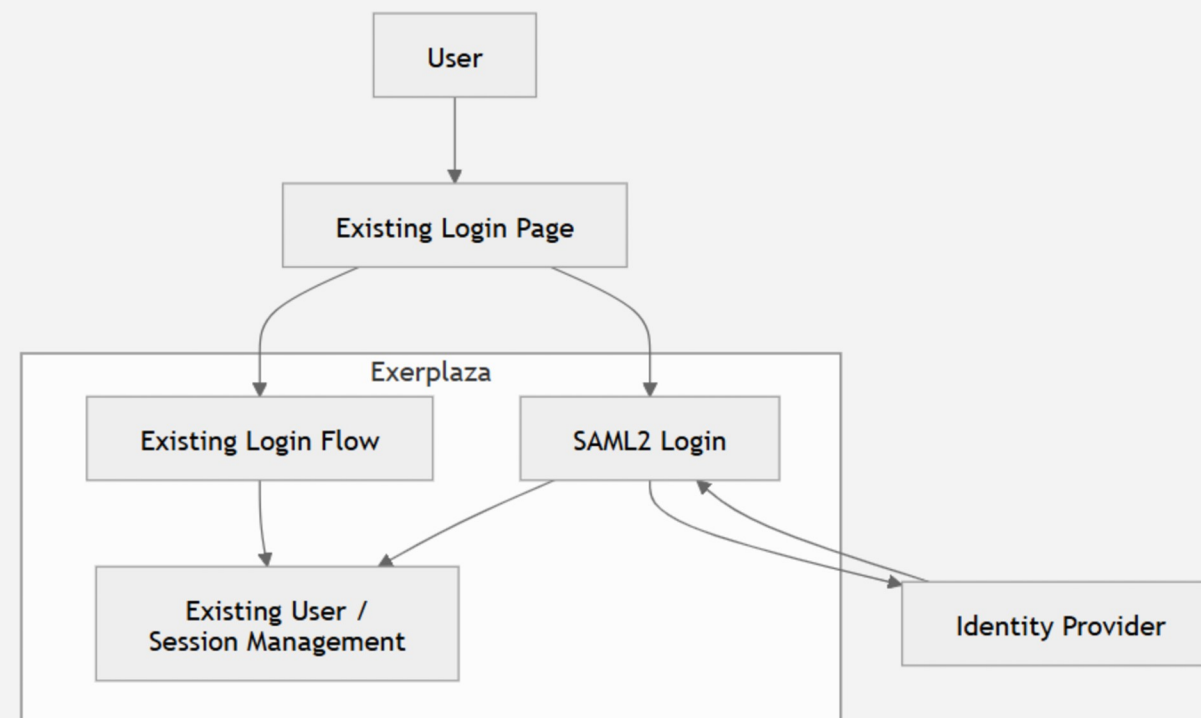
Email

Password

[Forgot password?](#)

[Sign in with Single Sign-On](#)

Need an account? [Sign up now](#)



Technical challenge: state across workers

Worker A:

- *Starts SSO login*
- *creates authentication request*
- *Stores request state locally*

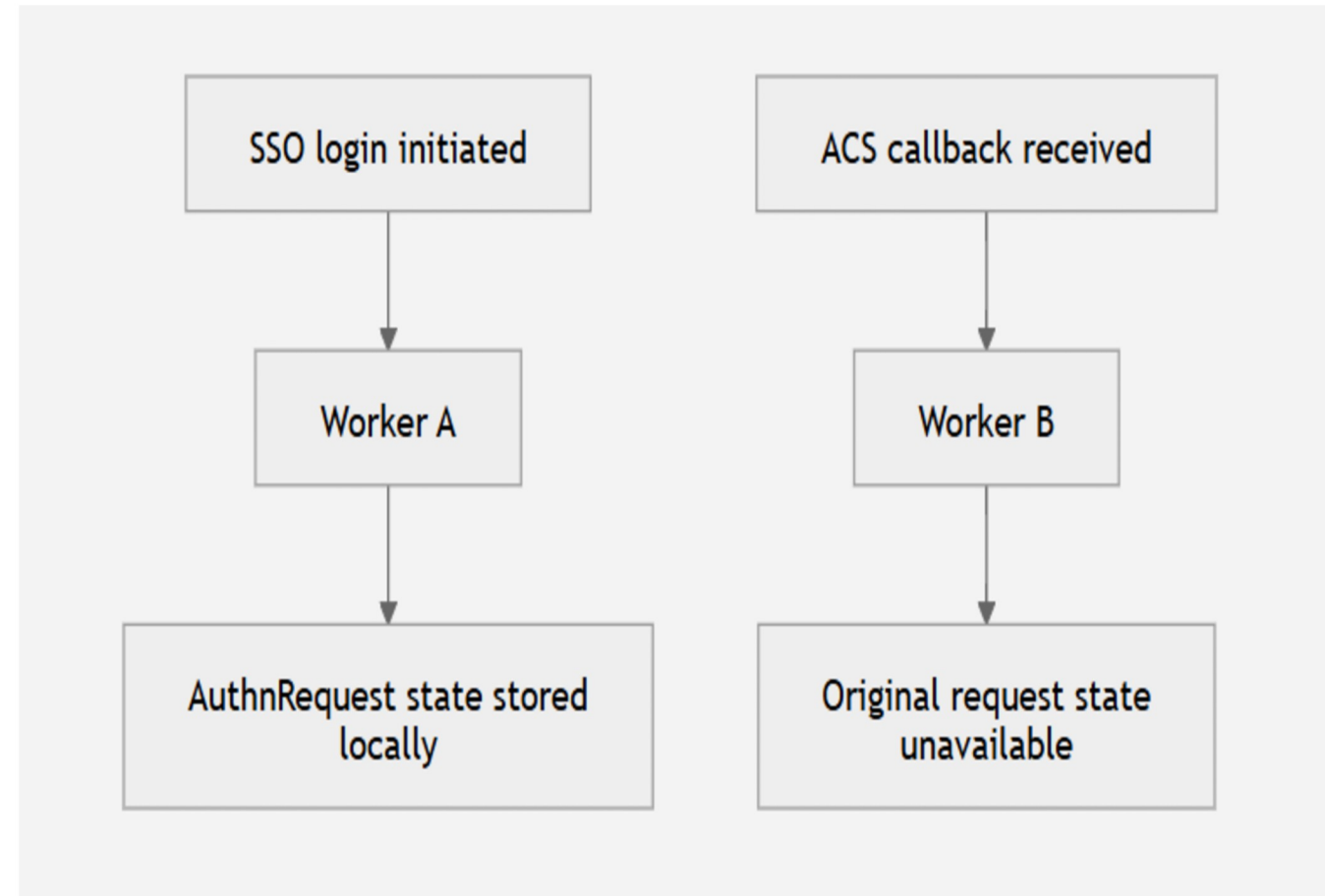
Identity provider:

- *Authenticates user*

Worker B:

- *Receives ACS callback*
- *Cannot recover original request state*
- *Valid authentication is rejected*

ACS = endpoint receiving the SAML response



THE SOLUTION

Database-backed request tracking

Login phase:

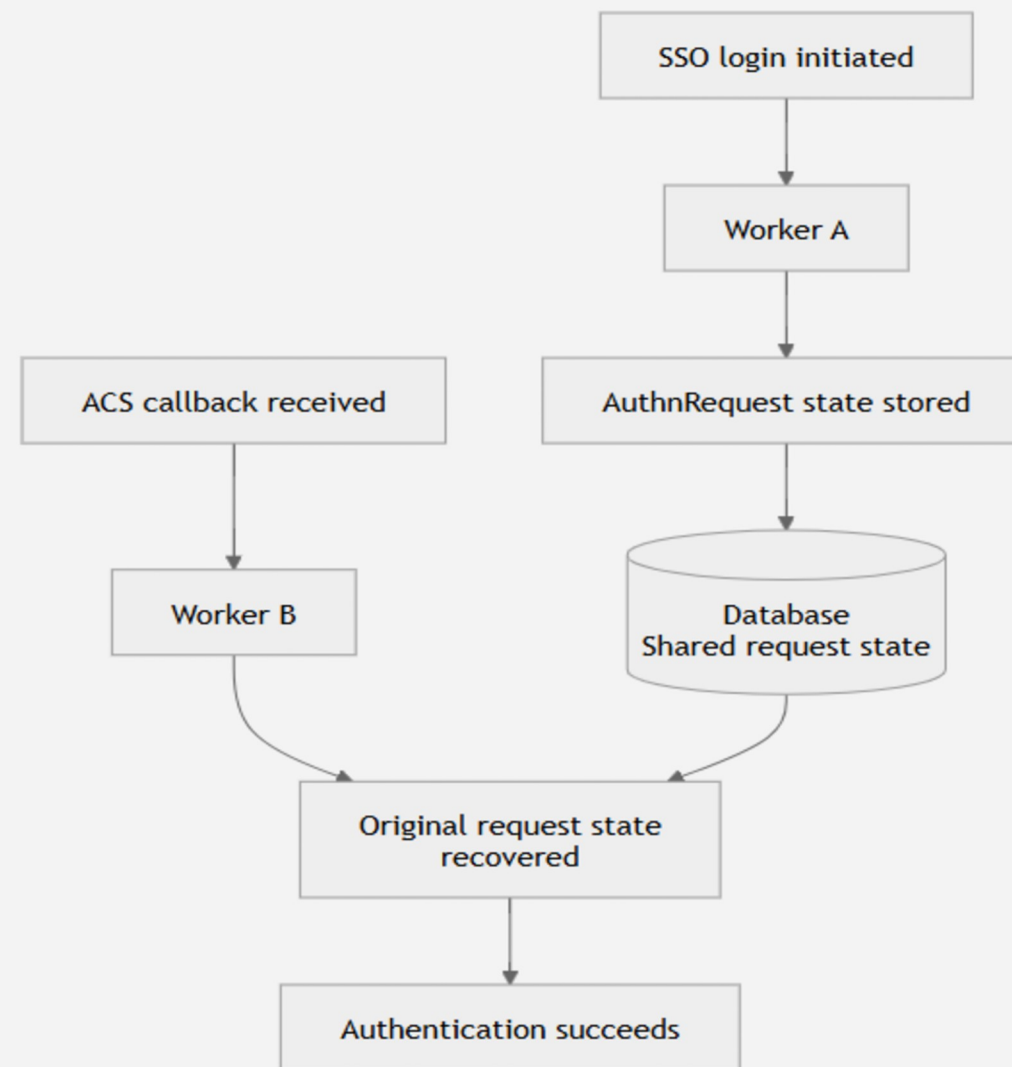
Worker A

- *Create Authentication Request*
- *Store request state in database*

ACS phase:

Worker B

- *Retrieve original request state*
- *Validate response*
- *Consume request after successful use*



Application integration tests

- *SAML routes and authentication behaviour*
- *Error handling and edge cases*
- *Database-backed request tracking*

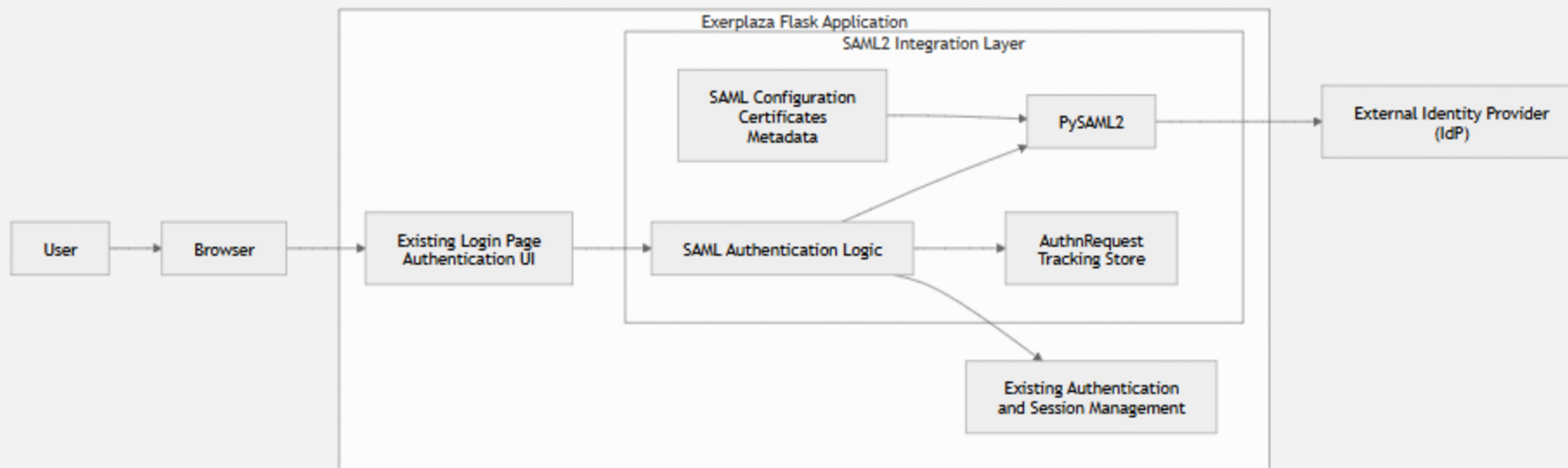
Security-related behaviour

- *One-time request consumption*
- *Replay prevention*
- *Redirect validation*

End-to-end validation

- *Complete SAML authentication flow*
- *Real Identity Provider integration*

FINAL OVERVIEW

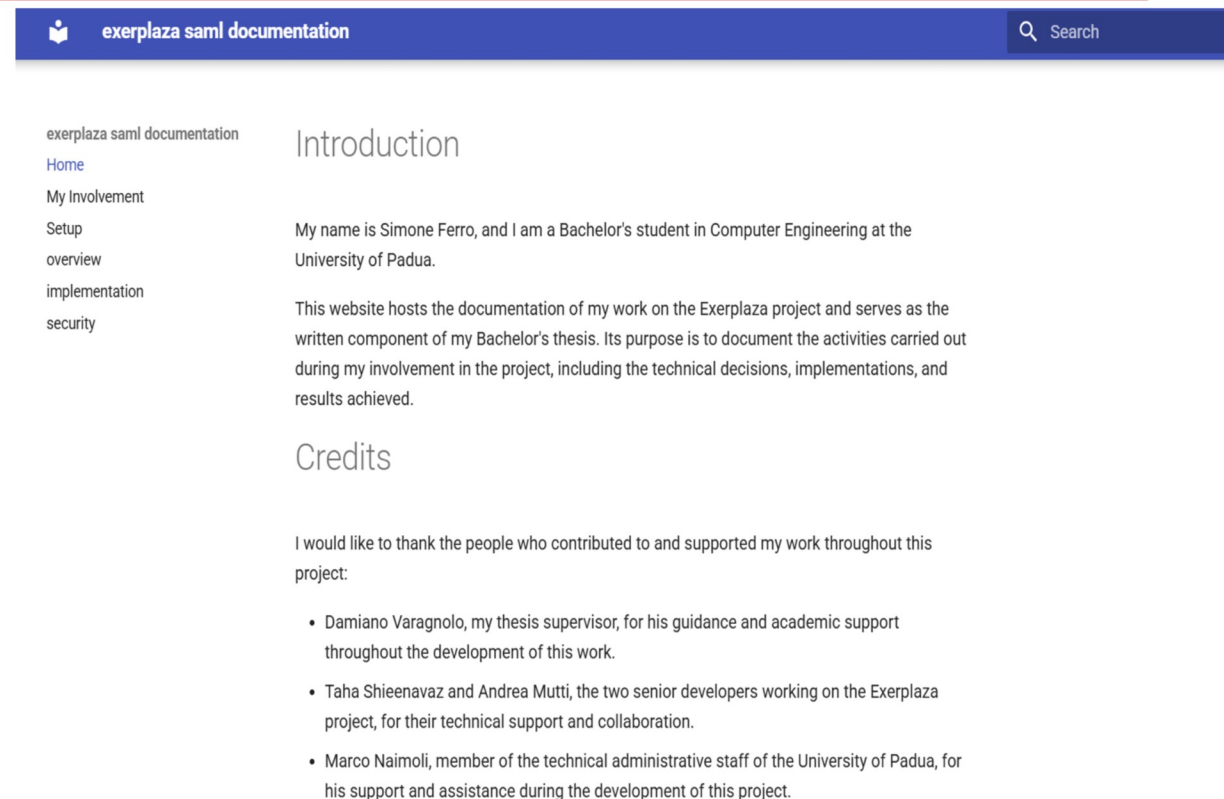


Documentation:

- *Dedicated website*
- *Architecture overview*
- *SAML2 authentication flow*
- *Configuration and deployment setup*
- *maintenance reference*

Code:

- *Improved separation and maintainability of Saml components*



The screenshot shows a web browser displaying the 'exerplaza saml documentation' website. The page has a blue header with the title and a search bar. A sidebar on the left contains a navigation menu with links: Home, My Involvement, Setup, overview, implementation, and security. The main content area is titled 'Introduction' and contains a paragraph about the author, Simone Ferro, a Bachelor's student in Computer Engineering at the University of Padua. It states that the website hosts documentation of his work on the Exerplaza project, which serves as the written component of his Bachelor's thesis. Below the introduction is a 'Credits' section where the author thanks several people: Damiano Varagnolo (thesis supervisor), Taha Shieenavaz and Andrea Mutti (senior developers), and Marco Naimoli (technical administrative staff). The page is well-structured and easy to navigate.

SAML2 integration achieved through:

- ✓Integration without replacing existing authentication*
- ✓Minimal hybrid architecture compatible with current workflow*
- ✓Reliable request tracking and validated authentication flow*

The implementation establishes a validated foundation for future SAML2 extension and further production hardening.

Documentation:

<https://acquanaturaleminerale.github.io/>